# PEDOMAN PRAKTIKUM UNTUK ANALISIS KEAMANAN JARINGAN KOMPUTER NIRKABEL DENGAN METODE *PROTECTED EXTENSIBLE AUTHENTICATION PROTOCOL* (PEAP) MENGGUNAKAN RADIUS


Oleh

Yosua John Muskitta

NIM : 6220009015


Skripsi ini telah diterima dan disahkan

Sebagai salah satu persyaratan guna memperoleh gelar

**SARJANA TEKNIK**


Program Studi Sistem Komputer

Fakultas Teknik Elektronika dan Komputer

Universitas Kristen Satya Wacana

Salatiga


Mei 2016

PERPUSTAKAAN UNIVERSITAS
UNIVERSITAS KRISTEN SATYA WACANA
Jl. Diponegoro 52 – 60 Salatiga 50711
Jawa Tengah, Indonesia
Telp. 0298 – 321212, Fax. 0298 321433
Email: library@staff.uksw.edu ; http://library.uksw.edu

# PERNYATAAN TIDAK PLAGIAT

Saya yang bertanda tangan di bawah ini:

Nama : YOSUA JOHN MUSKITTA

NIM : 672009015 Email : 672009015@student.uksw.edu

Fakultas : FTEK Program Studi : SISTEM KOMPUTER

Judul tugas akhir : PEDOMAN PRAKTIKUM UNTUK ANALISIS KEAMANAN JARINGAN KOMPUTER NIRKABEL DENGAN METODE PROTECTED EXTENSIBLE AUTHENTICATION PROTOCOL (PEAP) MENGGUNAKAN RADIUS

Pembimbing : 1. BANU WIRAWAN YOHANES, M.COMPSC.

2. HARTANTO KUSUMA WARDANA, M.T.

Dengan ini menyatakan bahwa:

1. Hasil karya yang saya serahkan ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar kesarjanaan baik di Universitas Kristen Satya Wacana maupun di institusi pendidikan lainnya.
2. Hasil karya saya ini bukan saduran/terjemahan melainkan merupakan gagasan, rumusan, dan hasil pelaksanaan penelitian/implementasi saya sendiri, tanpa bantuan pihak lain, kecuali arahan pembimbing akademik dan narasumber penelitian.
3. Hasil karya saya ini merupakan hasil revisi terakhir setelah diujikan yang telah diketahui dan disetujui oleh pembimbing.
4. Dalam karya saya ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali yang digunakan sebagai acuan dalam naskah dengan menyebutkan nama pengarang dan dicantumkan dalam daftar pustaka.

Pernyataan ini saya buat dengan sesungguhnya. Apabila di kemudian hari terbukti ada penyimpangan dan ketidakbenaran dalam pernyataan ini maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya saya ini, serta sanksi lain yang sesuai dengan ketentuan yang berlaku di Universitas Kristen Satya Wacana.

Salatiga, 13 JUNI 2016


YOSUA JOHN MUSKITTA

F-LIB-080

PERPUSTAKAAN UNIVERSITAS
UNIVERSITAS KRISTEN SATYA WACANA
Jl. Diponegoro 52 – 60 Salatiga 50711
Jawa Tengah, Indonesia
Telp. 0298 – 321212, Fax. 0298 321433
Email: library@adm.uksw.edu ; http://library.uksw.edu

# PERNYATAAN PERSETUJUAN AKSES

Saya yang bertanda tangan di bawah ini:

Nama : YOSUA JOHN MUSKITTA

NIM : 672009015 Email : 672009015@student.uksw.edu

Fakultas : FTEK Program Studi : SISTEM KOMPUTER

Judul tugas akhir : PEDOMAN PRAKTIKUM UNTUK ANALISIS KEAMANAN JARINGAN KOMPUTER NIRKABEL DENGAN METODE PROTECTED EXTENSIBLE AUTHENTICATION PROTOCOL (PEAP) MENGGUNAKAN RADIUS

Dengan ini saya menyerahkan hak *non-eksklusif** kepada Perpustakaan Universitas – Universitas Kristen Satya Wacana untuk menyimpan, mengatur akses serta melakukan pengelolaan terhadap karya saya ini dengan mengacu pada ketentuan akses tugas akhir elektronik sebagai berikut (beri tanda pada kotak yang sesuai):

☑ a. Saya mengijinkan karya tersebut diunggah ke dalam aplikasi Repositori Perpustakaan Universitas, dan/atau portal GARUDA

☐ b. Saya tidak mengijinkan karya tersebut diunggah ke dalam aplikasi Repositori Perpustakaan Universitas, dan/atau portal GARUDA**

* *Hak yang tidak terbatas hanya bagi satu pihak saja. Pengajar, peneliti, dan mahasiswa yang menyerahkan hak non-ekslusif kepada Repositori Perpustakaan Universitas saat mengumpulkan hasil karya mereka masih memiliki hak copyright atas karya tersebut.*

** *Hanya akan menampilkan halaman judul dan abstrak. Pilihan ini harus dilampiri dengan penjelasan/ alasan tertulis dari pembimbing TA dan diketahui oleh pimpinan fakultas (dekan/kaprodi).*

Demikian pernyataan ini saya buat dengan sebenarnya.

Salatiga, 13 JUNI 2016

YOSUA JOHN MUSKITTA
*Tanda tangan & nama terang mahasiswa*

Mengetahui,

Barry Wirawan Yohanes
*Tanda tangan & nama terang pembimbing I*

Hartanto Kusuma W
*Tanda tangan & nama terang pembimbing II*

F-LIB-081

**PEDOMAN PRAKTIKUM UNTUK ANALISIS KEAMANAN JARINGAN KOMPUTER NIRKABEL DENGAN METODE *PROTECTED EXTENSIBLE AUTHENTICATION PROTOCOL* (PEAP) MENGGUNAKAN RADIUS.**

Disusun Oleh

Yosua John Muskitta
NIM : 622009015

Skripsi ini telah diterima dan disahkan

sebagai salah satu persyaratan guna memperoleh gelar

SARJANA TEKNIK

dalam

Program Studi Sistem Komputer

FAKULTAS TEKNIK ELEKTRONIKA DAN KOMPUTER

UNIVERSITAS KRISTEN SATYA WACANA

SALATIGA

Disahkan Oleh

| Pembimbing I | Pembimbing II |
|---|---|
| **Banu W. Yohanes, M. CompSc.** | **Hartanto K. Wardana, M.T** |
| Tanggal : 14 Juni 2016 | Tanggal : 14 Juni 2016 |

# KATA PENGANTAR

Puji syukur penulis ucapkan kepada Tuhan Yesus atas segala berkat yang Ia berikan kepada penulis sehingga skripsi ini bisa diselesaikan sebagai syarat untuk menyelesaikan perkuliahan di Fakultas Teknik Elektronika dan Komputer Universitas Kristen Satya Wacana.

Ucapan terima kasih penulis ucapkan kepada semua pihak yang telah memberikan dukungan, bantuan, dan doa-doa selama penulis melaksanakan kuliah di Fakultas Teknik Elektronika dan Komputer Universitas Kristen Satya Wacana. Ucapan terima kasih penulis ucapkan kepada:

1. Keluarga tersayang, Papa (Lerry Steve Muskitta, M.sc), Mama (Jeine Soeratno), dan adik tercinta Yonatan Laurens Muskitta yang walaupun tidak bersama-sama tinggal dengan penulis tetap memberikan dukungan dengan semangat dan doa.
2. Bapak Banu Wirawan Yohanes, M.CompSc, selaku pembimbing I yang dengan sabar selalu membimbing penulis dalam proses perkuliahan dan proses skripsi.
3. Bapak Hartanto K. Wardhana, M.T, selaku pembimbing II dan wali studi yang selalu membantu penulis dalam proses perkuliahan, penulisan, dan evaluasi skripsi ini.
4. Seluruh Staff dosen dan tata usaha, Mba Yola, Mba Ragil, dan Mba Rista yang sudah membantu penulis dalam perkuliahan dan proses perkuliahan sampai pada proses skripsi.
5. Seluruh teman-teman elektro 2009, Codot, Abi, Edo, Adit, Pakde, Agung, Angel, Daniel, Gigih, Anne, dan teman-teman lain yang tidak bisa disebutkan satu per satu.
6. Seluruh teman-teman yang mengerjakan skripsi di BB5, Fredik, Sam, Anne, Adit, Kwang. Dan kepada Joshua Marthen Manuputty yang banyak membantu dalam proses Praktek Kerja dan Proses penyelesaian Skripsi.
7. Keluarga Pinaesaan Salatiga yang sudah menjadi keluarga kedua penulis selama proses perkuliahan di Salatiga.

8. Terima kasih sebesar-besarnya buat teman-teman terdekat penulis, Mayo BATMAN, Wakas, Carry, Caber, Jacques, Nani, Alen, Wate, Aney, Kris Monte, Sbot, Ciks, Tika, Regal, Theo, Eva, yang selalu setia bersama-sama dengan penulis dalam suka maupun duka.
9. Keluarga besa Fakultas Teknik Elektronika dan Komputer Universitas Kristen Satya Wacana sebagai tempat kuliah dan rumah kedua di Salatiga.
10. Semua pihak yang tidak dapat penulis sebutkan satu per satu. Yang sangat membantu penulis selama di Salatiga.

Akhir kata penulis memohon maaf jika skripsi ini belum sempurna dan masih banyak kekurangan. Dan semoga skripsi ini dapat berguna bagi pembaca untuk studi kedepanya.

Salatiga, April 2016

Penulis

# ABSTRACT

The development of wireless network has been made to replace wired network. Wireless network designed to broadcast their existance via beacon frames so that client can connect. Because of that wireless network has security problem. The students need for a guide that can help them to secure wireless network.

This thesis goal is to produce practical guidelines that will be used in the course of wireless network security. These practical guideliness that has been created consist of four guidelines i.e., introductions of wireless network, introduction and installation of remote access dial in user service (RADIUS), wireless security design using Protected Extensible Authentication Protocol (PEAP) method, dan wireless network attack test using dictionary attack. These guidelines purpose is that students can secure wireless network.

This thesis consists the analysis of PEAP method design and testing with dictionary attack. Dictionary attack will success if the passpharase is on the dictionary. PEAP method secures client identity. If the identity of client is listed on the dictionary, the identity cannot be cracking because it has been protected by PEAP.

**Keywords: Wireless Network, PEAP, Dictionary attack**

# INTISARI

Perkembangan dari teknologi jaringan nirkabel memungkinkan melakukan komunikasi tanpa harus dibatasi dengan panjangnya kabel. Dalam proses komunikasinya, jaringan nirkabel terus-menerus melakukan *broadcast* data sehingga semua *device* yang mendukung jaringan nirkabel bisa menginterupsi proses komunikasi tersebut. Hal ini dapat menimbulkan masalah keamanan. Oleh karena itu dibutuhkan suatu pedoman yang akan membantu mahasiswa untuk mempelajari dan mengamankan jaringan nirkabel.

Skripsi ini bertujuan untuk membuat pedoman praktikum yang akan digunakan pada matakuliah jaringan komputer. Pedoman praktikum yang telah dibuat terdiri dari 4 pedoman yaitu pengenalan jaringan nirkabel, pengenalan dan instalasi *Remote Access Dial In User Service* (RADIUS), pembuatan sistem keamanan jaringan nirkabel dengan metode *Protected extensible Authentication Protocol* (PEAP), dan pengujian jaringan nirkabel dengan metode *dictionary attack* menggunakan *aircrack-ng.*

Skripsi ini berisi mengenai analisa dari metode PEAP, mulai dari konfigurasi sampai dengan pengujian dengan menggunakan salah satu serangan pada jaringan nirkabel yaitu *dictionary attack.* Serangan *dictionary attack* dapat berhasil jika kata yang dicari ada di dalam kamus. Metode PEAP melindungi identitas klien sehingga walaupun identitas asli klien ada pada kamus, identitas klien tidak dapat dibaca karena identitas tersebut dilindungi oleh PEAP.

**Kata kunci: Jaringan Nirkabel, PEAP, *Dictionary Attack*.**

# DAFTAR ISI

# DAFTAR GAMBAR

# DAFTAR ISTILAH

| | |
|---|---|
| AAA | *Authentication, Authorization, Accounting* |
| AP | *Access Point* |
| DHCP | *Dynamic Host Configuration Protocol* |
| DNS | *Domain Name System* |
| EAP | *Extensible Authentication Protocol* |
| CHAP | *Challenge Handshake Authentication Protocol* |
| EAP-TLS | EAP-*Trasport Layer Security* |
| EAP-TTLS | EAP-*Tunneled Transport Layer Security* |
| EAPOL | *Extensible Authentication Protocol Over* LAN |
| IPv4 | *Internet Protocol version* 4 |
| IP | *Internet Protocol* |
| IETF | *Internet Engineering Task Force* |
| LAN | *Local Area Network* |
| OS | *Operating System* |
| PC | *Personal Computer* |
| PEAP | *Protected Extensible Authentication Protocol* |
| RADIUS | *Remote Authentication Dial In User Service* |
| IP | *Routing Information Protocol* |
| SSL | *Secure Socket Layer* |
| TCP | *Transmission Control Protocol* |
| TKIP | *Temporal Key Integrity Protocol* |

| | |
|---|---|
| UDP | *User Datagram Protocol* |
| WAN | *Wide Area Network* |
| WEP | *Wired Equivalent Privacy* |
| WPA | *Wi-fi Protected Access* |